#4

Docket No. 220944US2/btm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hisashi NAKAGOMI, et al. GAU: 2131

SERIAL NO: 10/098,575 EXAMINER:

FILED: March 18, 2002

FOR: MOBILE COMMUNICATION TERMINAL DEVICE AND SERVER DEVICE

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.
- ■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2001-078683	March 19, 2001

Certified copies of the corresponding Convention Application(s)

- ■ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
  Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
  (B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913
Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ３月１９日

出願番号
Application Number: 特願２００１－０７８６８３

[ST.10/C]: [ＪＰ２００１－０７８６８３]

出願人
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

２００２年 ４月 ２日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　12-0508
【提出日】　平成13年 3月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46
G06F 13/00
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　中込　寿
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　鷹見　忠雄
【特許出願人】
【識別番号】　392026693
【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ
【代理人】
【識別番号】　100088155
【弁理士】
【氏名又は名称】　長谷川　芳樹
【選任した代理人】
【識別番号】　100092657
【弁理士】
【氏名又は名称】　寺崎　史朗
【選任した代理人】
【識別番号】　100114270
【弁理士】
【氏名又は名称】　黒川　朋也

【選任した代理人】

【識別番号】　100108213

【弁理士】

【氏名又は名称】　阿部　豊隆

【選任した代理人】

【識別番号】　100113549

【弁理士】

【氏名又は名称】　鈴木　守

【手数料の表示】

【予納台帳番号】　014708

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　移動通信端末装置及びサーバ装置

【特許請求の範囲】

【請求項１】　セキュリティ通信機能を有する移動通信端末装置であって、

接続先のセキュリティレベルを検出する検出手段と、

前記検出されたセキュリティレベルを報知する報知手段とを備えることを特徴とする移動通信端末装置。

【請求項２】　前記検出されたセキュリティレベルが所定の条件を満足しているかどうかを判定する判定手段を更に備え、

前記報知手段は、前記判定結果を報知することを特徴とする請求項１記載の移動通信端末装置。

【請求項３】　通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なくとも一方を設定するセキュリティレベル設定手段を更に備えることを特徴とする請求項２記載の移動通信端末装置。

【請求項４】　前記検出されたセキュリティレベルが、前記通信を許容するセキュリティレベルに到達していない場合、又は前記通信を許容しないセキュリティレベルを下回る場合は、通信を停止する制御手段を更に備えることを特徴とする請求項３記載の移動通信端末装置。

【請求項５】　前記報知手段は、前記検出されたセキュリティレベルが、前記通信を許容するセキュリティレベルに到達していない場合、又は前記通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方の選択を催促することを特徴とする請求項３記載の移動通信端末装置。

【請求項６】　着信時に検出されたセキュリティレベルに基づいて通信を停止した場合は、発信元に対して通信を停止した旨を通知する通知手段を更に備えることを特徴とする請求項１記載の移動通信端末装置。

【請求項７】　通信ネットワークを介して移動通信端末装置と通信を行うサーバ装置であって、

セキュリティレベルを検出するサーバ側検出手段と、

通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベ

ルの少なくとも一方を設定するサーバ側セキュリティレベル設定手段とを備えることを特徴とするサーバ装置。

【請求項８】　前記検出されたセキュリティレベルが、前記通信を許容するセキュリティレベルに到達していない場合、又は前記通信を許容しないセキュリティレベルを下回る場合は、通信を停止するサーバ側制御手段を更に備えることを特徴とする請求項７記載のサーバ装置。

【請求項９】　前記検出されたセキュリティレベルが、前記通信を許容するセキュリティレベルに到達していない場合、又は前記通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方を選択するように前記移動通信端末装置に問い合わせる問い合わせ手段と、

前記問い合わせに対する応答に応じて通信を継続又は停止するサーバ側制御手段を更に備えることを特徴とする請求項７記載のサーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、セキュリティ通信機能を有する移動通信端末装置及びサーバ装置に関する。

【０００２】

【従来の技術】

従来から、無線通信システムにおいて、移動通信端末装置と通信システムとの間で通信の相手先の正当性を確認するための手段として、認証と呼ばれる通信手順が用いられている。また、移動通信端末装置と通信システムとの間で送受信される信号を暗号化するための手段として、秘匿と呼ばれる通信手順も併せて用いられている。これらの通信手順によって、移動通信端末装置と通信システムとが相互に通信の相手先の正当性を保証し、同時に伝送信号の秘密性を保持している。これにより、送信者又は受信者への成りすまし、データの改ざんや、盗み見などが防止されている。以上によって、通信及び通信システムのセキュリティが確保されている。

【０００３】

アナログ方式の無線通信システムにおいて、上記のようなセキュリティを確保するためには、アナログ無線変調の方式を変更する必要があった。このため、通信システム及び移動通信端末装置の変調及び復調回路に変調方式を変更するための回路を付加・増設しなければならなかった。その結果、通信システムコストが増大し、移動通信端末装置の回路増加に伴って消費電力が増大し、携帯性が著しく低下した。また、付加回路によるアナログ信号の演算過程の増加により通信信号の品質維持が容易でないという問題もあった。

【０００４】

その後、ディジタル方式の無線通信において、ディジタル信号処理による認証及び秘匿手段が提案され、セキュリティを確保することが容易となった。ただし、ディジタル方式を採る移動通信端末装置と通信システムとが接続する場合は、上記の認証及び秘匿に基づくセキュリティの確保が前提とされている。無線移動通信方式においては、電話呼の接続遅延は、サービス上、有線の電話接続と比較して長時間を要する設計にすることは望ましくない。また、データ通信において、インターネット接続におけるＷＷＷ利用などのインタラクティブな用途でも接続遅延はできるだけ小さいことが望ましい。このような要請に基づいて、移動通信端末装置と通信システムとの接続においては、接続開始から認証及び秘匿に要する時間が極力小さくなるように設計されている。

【０００５】

図１０は、現在移動通信システムと移動通信端末装置との接続の際に用いられている認証及び秘匿の通信手順の例を示す図である。図１０に示すように、待ち受け状態から無線チャネル接続手順が開始された後、通信システムから移動通信端末装置へ認証要求がなされる。移動通信端末装置は、認証要求を受けると通信システムに対して認証応答を行う。次に、通信システムは、移動通信端末装置へ秘匿要求を行い、これに対して移動通信端末装置は秘匿応答を行う。次に、回線接続手順が開始され、通信確立状態へ移行する。このように、認証及び秘匿は、少ない信号の送受信で完了する設計となっている。従って、使用者は、着信又は発信の操作の際、認証及び秘匿の通信手順の内容や状態について認識する必要がなく、直ちに通信を行うことが可能となっている。

【０００６】

今後、伝送速度がより高速化し、従来の音声通信やデータ通信に加えて、移動通信端末装置によって電子商取引や有料コンテンツ情報の配信サービスなどの実現が想定される。このように多様化した通信では、次のような内容のセキュリティが求められている。

① 従来どおりの移動通信端末装置及び通信システム間のセキュリティの提供。

② 金融機関、クレジットカード会社などとの取引き情報等、移動通信端末装置とインターネットなどで接続された通信の相手先までのエンドトゥエンドのセキュリティの提供。

【０００７】

これらを同時に満たすためには、現在用いることができる最も強力とされるセキュリティ技術に基づいたハードウェア及びソフトウェアを通信システムと移動通信端末装置がすべて搭載すれば良いと考えることもできる。

【０００８】

【発明が解決しようとする課題】

しかし、機能及び強度がより高いとされるセキュリティにおいては、認証及び秘匿における演算処理が増大して、接続遅延が増大する。また、伝送データの暗号化処理負荷の増大により通信システムの処理能力を圧迫し、移動通信端末の消費電力の増加を招くことがある。

【０００９】

このため、通信の伝送速度、通信の相手先（電話、通信システムと接続された相手先のサーバなど、相手のセキュリティ能力による）、通信の種類に適したセキュリティの機能及び強度（セキュリティレベル）、セキュリティ手順の処理時間及び負荷のトレードオフとして、適用するセキュリティを適切に選択できることが求められる。

【００１０】

さらに、特定の条件下でセキュリティの提供が行われない場合（地域、国家、通信システムの負荷低減などの運用条件、移動通信端末の信号処理を簡素化して消費電力の削減を行う場合など）において、セキュリティの提供が行われない場

合が想定される。このように、移動通信端末装置及び移動無線通信システムにおけるセキュリティレベルは多様化する。

【００１１】

本発明は、このような事情に鑑みてなされたものであり、接続先のセキュリティレベルに応じて接続可否を選択することができる移動通信端末装置及びサーバ装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】

上記の目的を達成するため、請求項１記載の移動通信端末装置の発明は、セキュリティ通信機能を有する移動通信端末装置であって、接続先のセキュリティレベルを検出する検出手段と、検出されたセキュリティレベルを報知する報知手段とを備える構成を採る。

【００１３】

このように、通信を行うに際し、接続先のセキュリティレベルを検出し、検出したセキュリティレベルを報知するので、使用者は、接続先においてセキュリティが確保されているかどうかを確認することが可能となる。ここで、通信とは、音声通信、データ通信などの通常の通信のみならず、移動通信端末装置の位置情報通知等の制御用通信も含む意味である。

【００１４】

請求項２記載の発明は、請求項１記載の移動通信端末装置において、検出されたセキュリティレベルが所定の条件を満足しているかどうかを判定する判定手段を更に備え、報知手段は、判定結果を報知する構成を採る。

【００１５】

このように、検出されたセキュリティレベルが所定の条件を満足しているかどうかを判定するので、使用者は、判定結果に応じて通信を継続するか又は停止するかを選択することが可能となる。

【００１６】

請求項３記載の発明は、請求項２記載の移動通信端末装置において、通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なく

とも一方を設定するセキュリティレベル設定手段を更に備える構成を採る。

【００１７】

この構成により、使用者の判断で、必要なセキュリティレベルを自由に設定することができる。

【００１８】

請求項４記載の発明は、請求項３記載の移動通信端末装置において、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する制御手段を更に備える構成を採る。

【００１９】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する。これにより、使用者が設定したセキュリティの条件を満足していない場合は、通信を自動的に停止することができ、セキュリティに関するトラブルの発生を未然に防止することができる。

【００２０】

請求項５記載の発明は、請求項３記載の移動通信端末装置において、報知手段は、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方の選択を催促する構成を採る。

【００２１】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方の選択を催促する。これにより、使用者は、検出されたセキュリティレベルが、設定した条件を満足しない場合は、通信を継続するか停止するかを選択することが可能となる。

【００２２】

請求項６記載の発明は、請求項１記載の移動通信端末装置において、着信時に検出されたセキュリティレベルに基づいて通信を停止した場合は、発信元に対し

て通信を停止した旨を通知する通知手段を更に備える構成を採る。

【００２３】

このように、着信時に検出されたセキュリティレベルに基づいて通信を停止した場合は、発信元に対して通信を停止した旨を通知する。これにより、発信元に対して通信を停止した旨を知らしめることが可能となる。

【００２４】

請求項７記載のサーバ装置の発明は、通信ネットワークを介して移動通信端末装置と通信を行うサーバ装置であって、セキュリティレベルを検出するサーバ側検出手段と、通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なくとも一方を設定するサーバ側セキュリティレベル設定手段とを備える構成を採る。

【００２５】

この構成により、使用者の判断で、必要なセキュリティレベルを自由に設定することができる。

【００２６】

請求項８記載の発明は、請求項７記載のサーバ装置において、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止するサーバ側制御手段を更に備える構成を採る。

【００２７】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する。これにより、使用者が設定したセキュリティの条件を満足していない場合は、通信を自動的に停止することができ、セキュリティに関するトラブルの発生を未然に防止することができる。

【００２８】

請求項９記載の発明は、請求項７記載のサーバ装置において、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止

のいずれか一方を選択するように移動通信端末装置に問い合わせる問い合わせ手段と、問い合わせに対する応答に応じて通信を継続又は停止するサーバ側制御手段を更に備える構成を採る。

【００２９】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方を選択するように移動通信端末装置に問い合わせを行い、問い合わせに対する応答に応じて通信を継続又は停止する。これにより、使用者は、検出されたセキュリティレベルが、設定した条件を満足しない場合は、通信を継続するか停止するかを選択することが可能となる。

【００３０】

【発明の実施の形態】

図１は、本発明の実施の形態に係る移動通信端末装置の概略構成を示すブロック図である。移動通信端末装置１は、セキュリティ通信機能を有しており、アンテナ２を備える無線部３によって無線通信を行う。セキュリティレベル検出手段４は、接続先のセキュリティレベルを検出し、報知手段５は、検出されたセキュリティレベルを使用者に対して報知する。この報知は、例えば、図示しない液晶画面にセキュリティレベルをグラフ状に表示しても良いし、音声データを出力することにより行っても良い。

【００３１】

判定手段６は、セキュリティレベル検出手段４によって検出されたセキュリティレベルが所定の条件を満足しているかどうかを判定する。所定の条件としては、例えば、後述するセキュリティレベル設定手段７を介して使用者によって設定されたセキュリティレベルや、予め定められているセキュリティレベルなどがある。報知手段５は、判定結果を使用者に対して報知する。これにより、使用者は、通信に際してセキュリティが確保されているかどうかを認識することが可能となる。

【００３２】

セキュリティレベル設定手段７は、通信を許容するセキュリティレベル、又は

通信を許容しないセキュリティレベルの少なくとも一方を設定する。これにより、使用者の判断で、必要なセキュリティレベルを自由に設定することができる。制御手段８は、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する。これにより、トラブルが生ずる可能性が高いと考えられる通信を回避することができる。通知手段９は、着信時に検出されたセキュリティレベルに基づいて通信を停止した場合は、発信元に対して通信を停止した旨を通知する。以上の各構成要素は、制御バス１０によって相互に接続されている。

【００３３】

なお、報知手段５は、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方の選択を催促しても良い。

【００３４】

図２は、本発明の実施の形態に係るサーバ装置の概略構成を示す図である。サーバ装置２０は、ネットワークインタフェース２１を介して通信ネットワークと接続されており、図示しない交換機及び基地局を介して移動通信端末装置と通信を行う。サーバ側検出手段２２は、移動通信端末装置による通信のセキュリティレベルを検出し、サーバ側セキュリティレベル設定手段２３は、使用者の指示に基づいて、通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なくとも一方を設定する。サーバ側制御手段２４は、サーバ側検出手段２２により検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する。これにより、トラブルが生ずる可能性が高いと考えられる通信を回避することができる。

【００３５】

問い合わせ手段２５は、サーバ側検出手段２２により検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信

を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方を選択するように移動通信端末装置に問い合わせを行い、サーバ側制御手段２４は、問い合わせに対する応答に応じて通信を継続又は停止する。

【００３６】

図３は、本発明の実施の形態に係る通信システムの概略を示す図である。移動通信端末装置としての携帯電話装置３０は、図１に示した基本構成を採っており、さらにセキュリティ情報を格納した内部メモリと、外部通知用インタフェースを備えている。携帯電話装置３０は、基地局３１と無線により信号の送受信を行う。携帯電話装置３０が送信した信号は、基地局３１により受信され、交換機３２を介してコアネットワーク３３に接続されているサーバ装置としての使用者情報サーバ３４に伝送される。使用者情報サーバ３４は、図２に示した基本構成を採っており、さらにセキュリティ情報を格納した内部メモリと、使用者ＩＤとを備えている。使用者情報サーバ３４が送信した信号は、この逆の流れで携帯電話装置３０に伝送される。

【００３７】

次に、以上のように構成された本発明の実施の形態に係る通信システムの動作について説明する。図４は、移動通信端末装置の動作を示すフローチャートである。移動通信端末装置に着信があった場合、又は移動通信端末装置が発信を行った場合（ステップＳ１）、移動通信端末装置と通信システムとは通信起動手順を開始する（ステップＳ２）。次に、その通信又は通信システムのセキュリティレベルが検出され、その情報が交換されて、使用者に通知される（ステップＳ３）。その後、通信が確立される（ステップＳ４）。ここで、使用者への通知方法としては、図３に示した外部通信用インタフェースとして、移動通信端末装置の画面上で、例えば、液晶ディスプレイ、発光素子の点灯、点滅又は色彩の変更等を行っても良い。また、音声トーキー及び振動等による通知を行っても良い。ここでは、移動通信端末装置への通知に止めておき、使用者には直接通知しない形態を採っても良い。

【００３８】

このように、通信を行うに際し、接続先のセキュリティレベルを検出し、検出

したセキュリティレベルを報知するので、使用者は、接続先においてセキュリティが確保されているかどうかを確認することが可能となる。

【００３９】

図５は、移動通信端末装置の他の動作を示すフローチャートである。移動通信端末装置に着信があった場合、又は移動通信端末装置が発信を行った場合（ステップＴ１）、移動通信端末装置と通信システムとは通信起動手順を開始する（ステップＴ２）。次に、その通信又は通信システムのセキュリティレベルが検出され、その情報が交換されて、使用者に通知される（ステップＴ３）。使用者は、外部通知用インタフェース等を介してその通知を認識し、通信を継続するか切断するかを選択する（ステップＴ４）。切断が選択された場合は、通信は終了し（Ｔ５）、継続が選択された場合は、通信が確立される（ステップＴ６）。

【００４０】

このように、検出されたセキュリティレベルが所定の条件を満足しているかどうかを判定するので、使用者は、判定結果に応じて通信を継続するか又は停止するかを選択することが可能となる。

【００４１】

図６は、移動通信端末装置の他の動作を示すフローチャートである。使用者は、移動通信端末装置内のセキュリティレベル情報を格納する内部メモリ、又は通信システム内の使用者情報サーバにおけるセキュリティレベル情報を格納する内部メモリに予めセキュリティ条件を設定する（ステップＲ１）。ここでは、通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なくとも一方を設定することが可能である。移動通信端末装置に着信があった場合、又は移動通信端末装置が発信を行った場合（ステップＲ２）、移動通信端末装置と通信システムとは通信起動手順を開始する。次に、その通信又は通信システムのセキュリティレベルを検出し、検出したセキュリティレベルと、使用者が予め設定したセキュリティレベル条件とを比較し（ステップＲ３）、条件を満たさない場合は、通信を切断する（ステップＲ４）。一方、条件を満たす場合は、通信を確立する（ステップＲ５）。

【００４２】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信を停止する。これにより、使用者が設定したセキュリティの条件を満足していない場合は、通信を自動的に停止することができ、セキュリティに関するトラブルの発生を未然に防止することができる。

【００４３】

図７は、移動通信端末装置の他の動作を示すフローチャートである。使用者は、移動通信端末装置内のセキュリティレベル情報を格納する内部メモリ、又は通信システム内の使用者情報サーバにおけるセキュリティレベル情報を格納する内部メモリに予めセキュリティ条件を設定する（ステップＰ１）。ここでは、通信を許容するセキュリティレベル、又は通信を許容しないセキュリティレベルの少なくとも一方を設定することが可能である。移動通信端末装置に着信があった場合、又は移動通信端末装置が発信を行った場合（ステップＰ２）、移動通信端末装置と通信システムとは通信起動手順を開始する（ステップＰ３）。次に、その通信又は通信システムのセキュリティレベルを検出し、検出したセキュリティレベルと、使用者が予め設定したセキュリティレベル条件とを比較し（ステップＰ４）、条件を満たさない場合は、使用者に対し、通信の継続又は切断の選択を促し、いずれが選択されたのかを判断する（ステップＰ５）。切断が選択された場合は通信が切断され（ステップＰ６）、継続が選択された場合は、通信が確立される（ステップＰ７）。一方、ステップＰ４において、セキュリティ条件が満たされている場合は、通信が確立される（ステップＰ８）。

【００４４】

このように、検出されたセキュリティレベルが、通信を許容するセキュリティレベルに到達していない場合、又は通信を許容しないセキュリティレベルを下回る場合は、通信の継続又は停止のいずれか一方の選択を催促する。これにより、使用者は、検出されたセキュリティレベルが、設定した条件を満足しない場合は、通信を継続するか停止するかを選択することが可能となる。

【００４５】

図８は、移動通信端末装置の他の動作を示すフローチャートである。通信の相

手側から移動通信端末装置に着信があった場合（ステップＹ１）、移動通信端末装置と通信システムとは通信起動手順を開始する。次に、その通信又は通信システムのセキュリティレベルによる接続判断を行い（ステップＹ２）、接続可能であるかどうかを判断する（ステップＹ３）。接続可能でない場合は、相手側にセキュリティレベルによって接続を停止したことを通知し（ステップＹ４）、通信を切断する（ステップＹ５）。一方、ステップＹ３において、接続可能である場合は、通信を確立する（ステップＹ６）。

【００４６】

このように、着信時に検出されたセキュリティレベルに基づいて通信を停止した場合は、発信元に対して通信を停止した旨を通知する。これにより、発信元に対して通信を停止した旨を知らしめることが可能となる。

【００４７】

図９は、本発明に係る通信システムの変形例を示す図である。この例では、図３に示す通信システムに加え、コアネットワーク３３には他のネットワーク３５が接続されており、さらに、コアネットワーク３３には交換機３６を介して基地局３７が接続されている。基地局３７は、相手側通信端末装置３８と無線通信を行う。この例では、使用者は、使用者が有する携帯電話装置３０から接続する相手側通信端末装置３８までの経路のセキュリティを確認することが可能である。また、使用者がセキュリティレベルを確認する方法、及び相手側への通知方法としては、音声通信の場合は音声トーキーや移動通信端末装置への画面表示等が考えられる。また、データ通信の場合は、ＡＴコマンド、移動通信端末装置への画面表示、通信を行っているアプリケーション上でのアラーム表示等が考えられる。また、人間が介在しない通信、例えば、自動販売機等に設置された移動通信端末装置とホストコンピュータとの通信の場合は、人間が直接確認することができないため、通信を行っているソフトウェアがその確認を行ったり、アラームを記録することが考えられる。

【００４８】

なお、以上の説明において、使用者がセキュリティレベルを確認する情報として、セキュリティの提供方式、例えば、秘匿のみ、認証のみ、暗号強度の差など

が考えられる。下記の表１は、通知方法の例を示す。表１において、「ＵＥ」とは、Ｕｓｅｒ　Ｅｑｕｉｐｍｅｎｔ（移動通信端末装置）を意味する。「ＮＷ」とは、Ｎｅｔｗｏｒｋ（ネットワーク）を意味し、「通信システム」、「通信」の意味を含む。

【００４９】

【表１】

セキュリティなしのネットワークでのＵＥ動作と表示	発信時	着信時	発信元へのＮＷトーキー等
使用者による選択あり	電話番号入力後、オフフック時にダイアログでそのまま発信するかどうかを確認	着信中にダイアログ表示をし、そのまま着信するかどうかを確認	使用者により通信の継続を停止した旨を通知
使用者による選択なし	発信無効“セキュリティなしＮＷ”	着信無効“セキュリティなしＮＷ”	ＤＩＳＣＯＮＮＥＣＴ使用者拒否

このように、本実施の形態によれば、使用者は、接続を試みている通信又は通信システムのセキュリティレベルを確認することができるため、接続をするかどうかを選択することができ、通信のセキュリティを確保することが可能となる。

【００５０】

【発明の効果】

以上説明したように、本発明に係る移動通信端末装置は、セキュリティ通信機能を有する移動通信端末装置であって、接続先のセキュリティレベルを検出する検出手段と、検出されたセキュリティレベルを報知する報知手段とを備える構成を採る。

【００５１】

このように、通信を行うに際し、接続先のセキュリティレベルを検出し、検出したセキュリティレベルを報知するので、使用者は、接続先においてセキュリティが確保されているかどうかを確認することが可能となる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係る移動通信端末装置の概略構成を示すブロック図である。

【図２】

本発明の実施の形態に係るサーバ装置の概略構成を示す図である。

【図３】

本発明の実施の形態に係る通信システムの概略を示す図である。

【図４】

移動通信端末装置の動作を示すフローチャートである。

【図５】

移動通信端末装置の他の動作を示すフローチャートである。

【図６】

移動通信端末装置の他の動作を示すフローチャートである。

【図７】

移動通信端末装置の他の動作を示すフローチャートである。

【図８】

移動通信端末装置の他の動作を示すフローチャートである。

【図９】

本発明に係る通信システムの変形例を示す図である。

【図１０】

現在移動通信システムと移動通信端末装置との接続の際に用いられている認証及び秘匿の通信手順の例を示す図である。

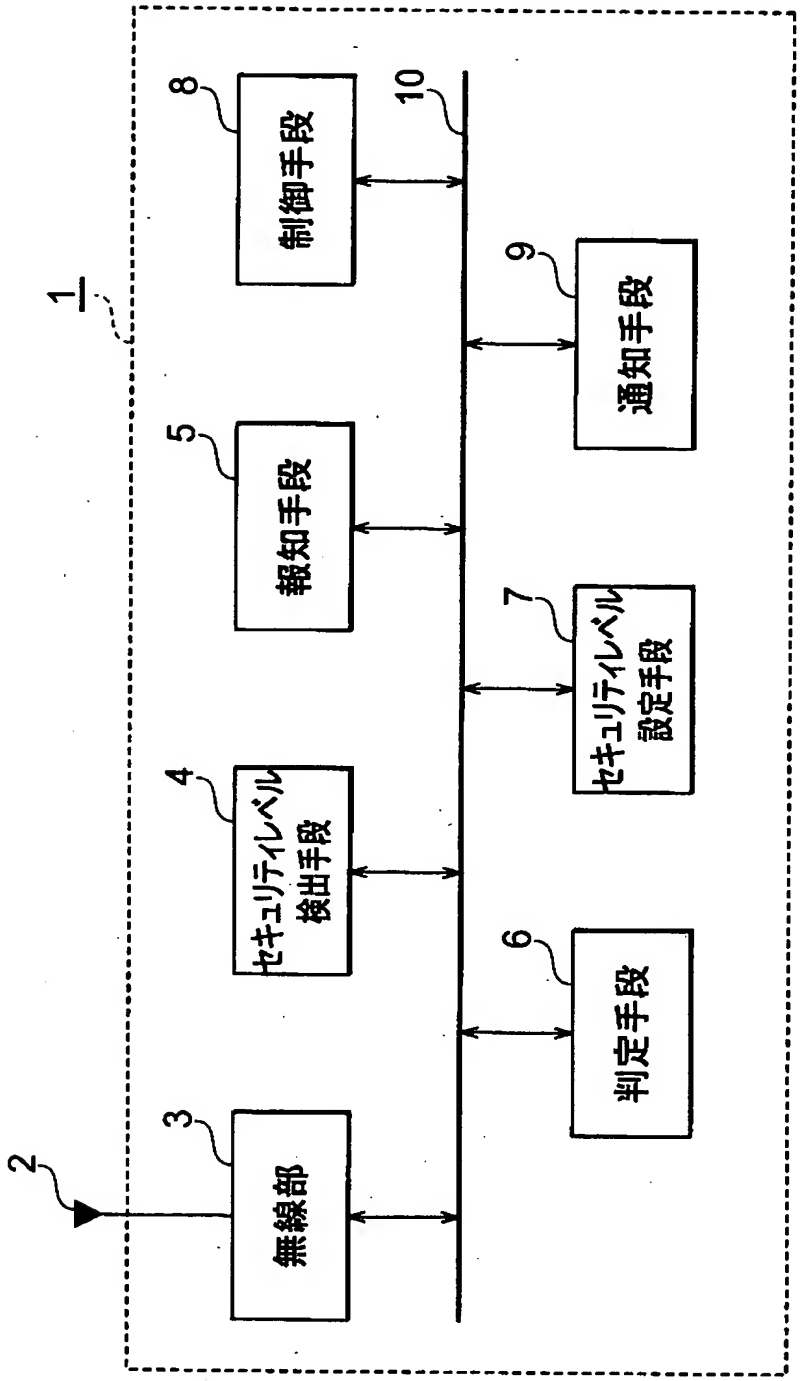
【符号の説明】

１…移動通信端末装置、２…アンテナ、３…無線部、４…セキュリティレベル検出手段、５…報知手段、６…判定手段、７…セキュリティレベル設定手段、８…制御手段、９…通知手段、１０…制御バス、２０…サーバ装置、２１…ネットワークインタフェース、２２…サーバ側検出手段、２３…サーバ側セキュリティレベル設定手段、２４…サーバ側制御手段、２５…問い合わせ手段、３０…携帯電話装置、３１…基地局、３２…交換機、３３…コアネットワーク、３４…使用者情報サーバ、３５…他のネットワーク、３６…交換機、３７…基地局、３８…

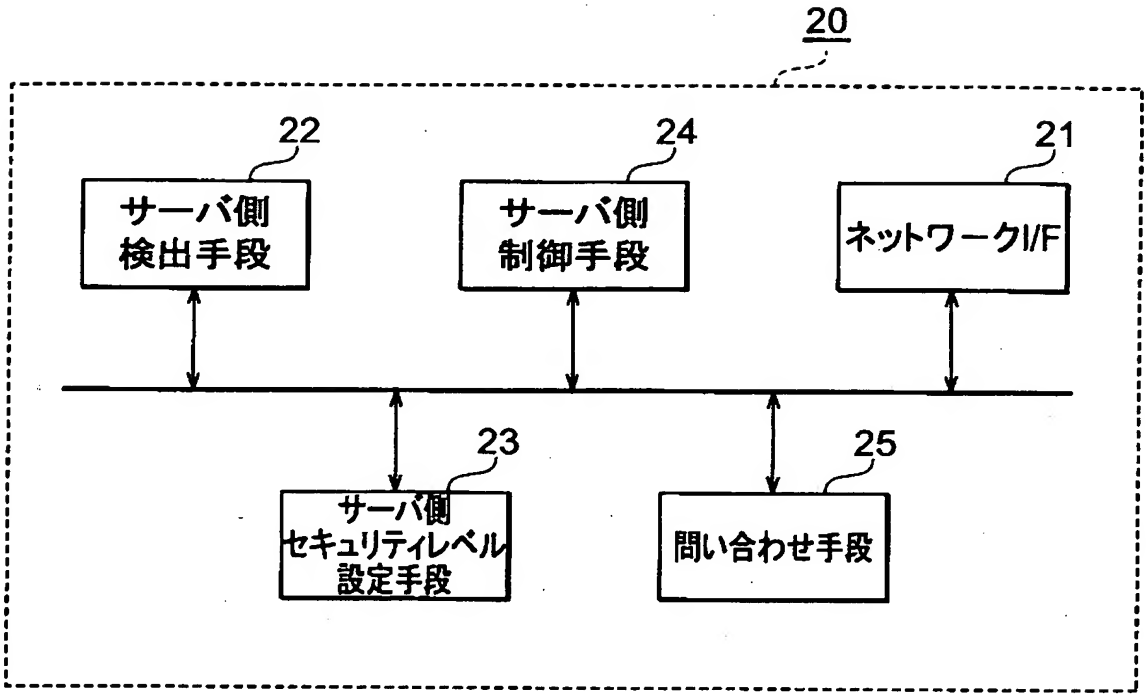
相手側通信端末装置。

【書類名】　　図面

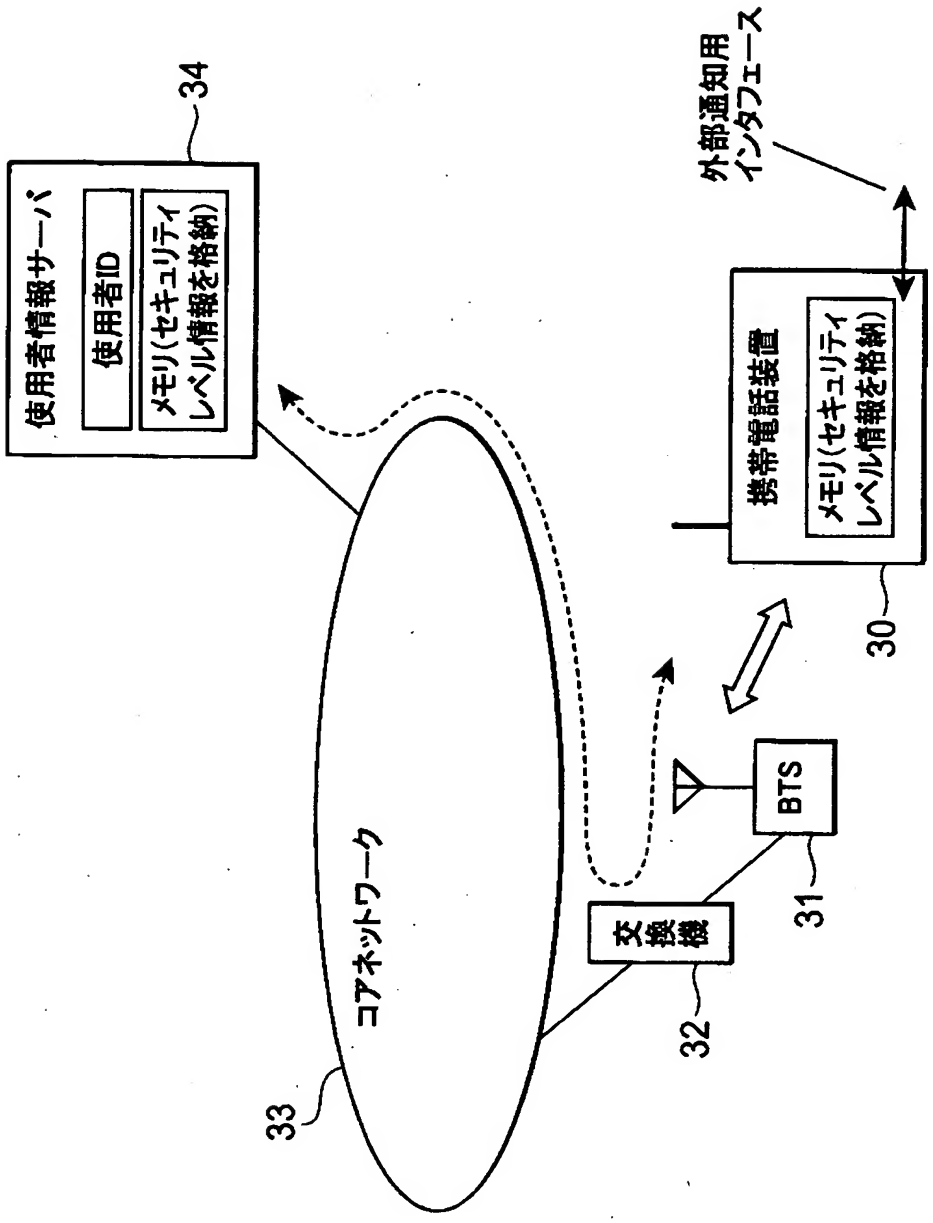
【図１】


1
2
3
無線部
4
セキュリティレベル検出手段
5
報知手段
6
判定手段
7
セキュリティレベル設定手段
8
制御手段
9
通知手段
10

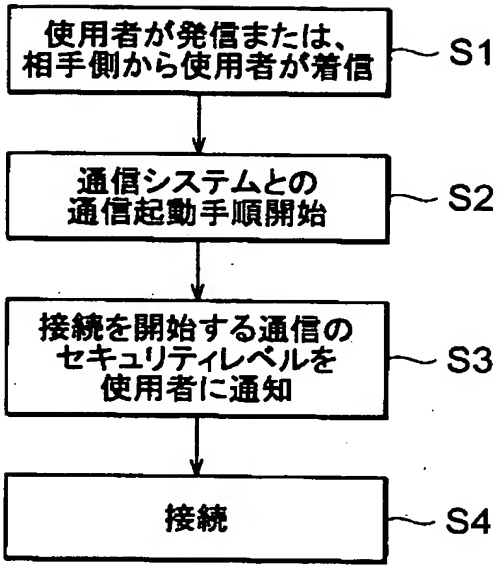
【図２】


20
22
サーバ側
検出手段
24
サーバ側
制御手段
21
ネットワークI/F
23
サーバ側
セキュリティレベル
設定手段
25
問い合わせ手段

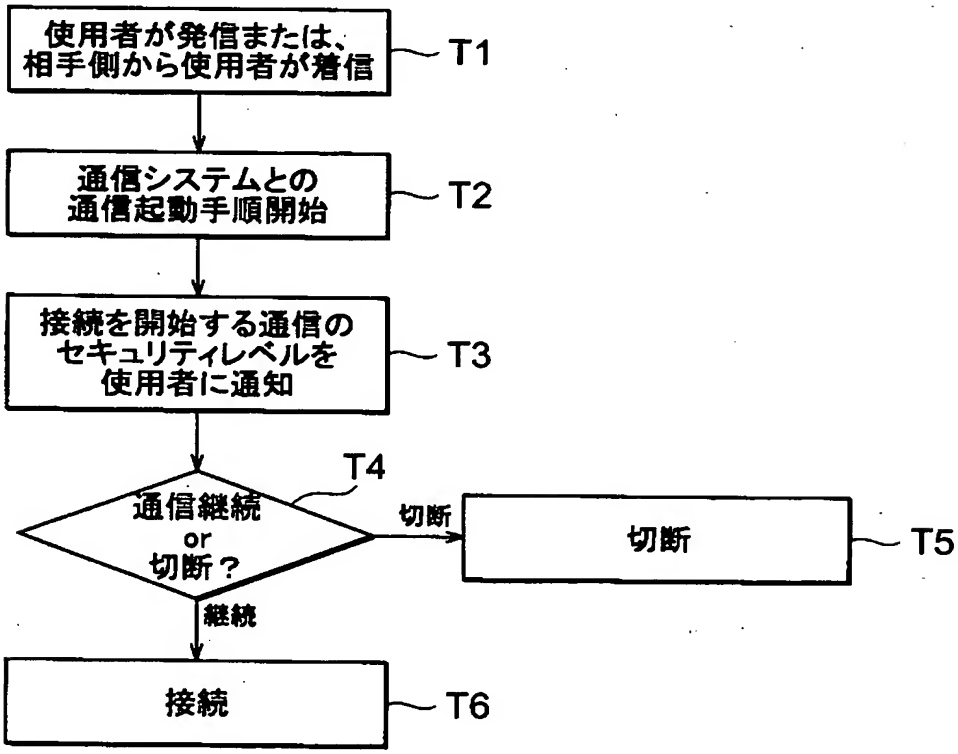
【図３】


34
使用者情報サーバ
使用者ID
メモリ(セキュリティレベル情報を格納)
外部通知用インタフェース
携帯電話装置
メモリ(セキュリティレベル情報を格納)
30
BTS
31
交換機
32
コアネットワーク
33

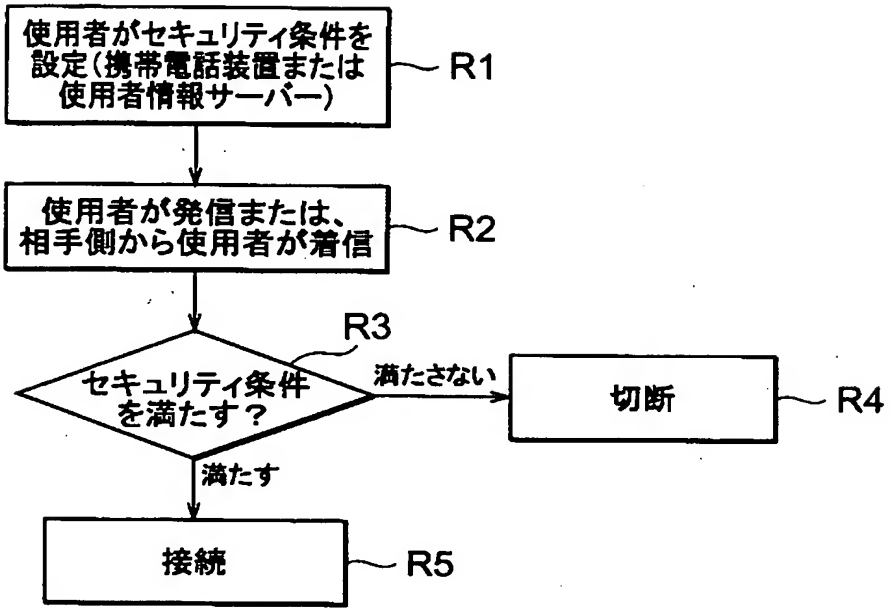
【図４】


使用者が発信または、
相手側から使用者が着信
S1
通信システムとの
通信起動手順開始
S2
接続を開始する通信の
セキュリティレベルを
使用者に通知
S3
接続
S4

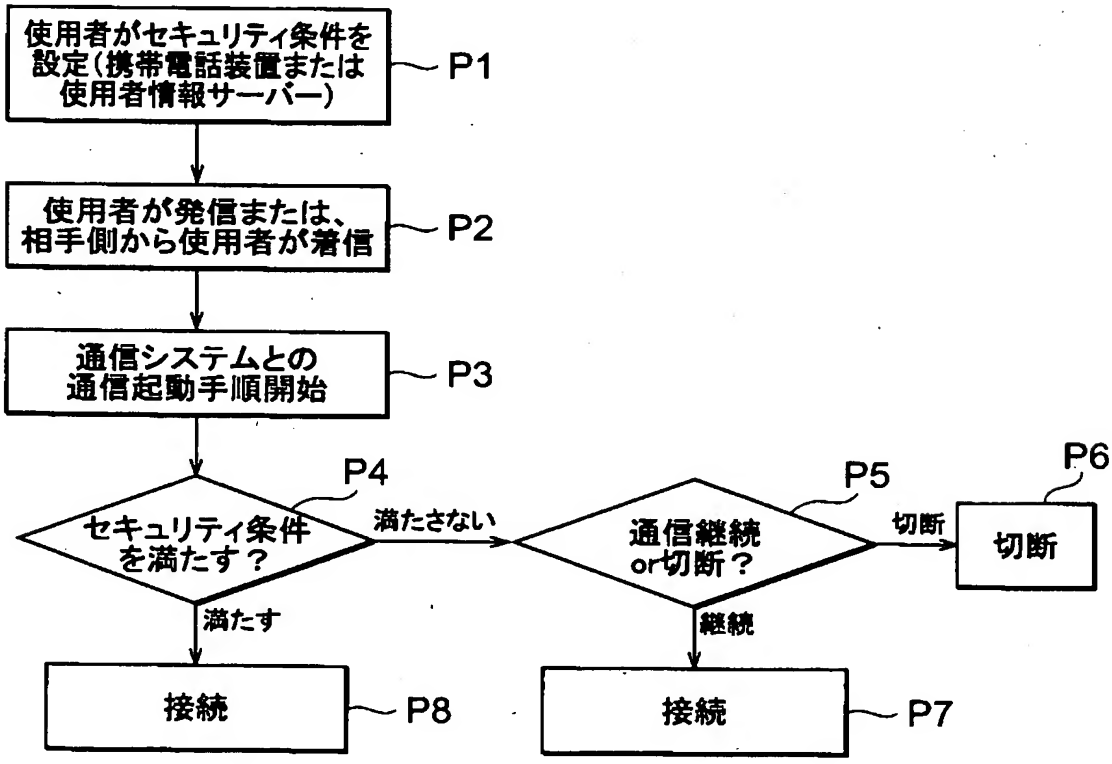
【図５】


使用者が発信または、
相手側から使用者が着信
T1
通信システムとの
通信起動手順開始
T2
接続を開始する通信の
セキュリティレベルを
使用者に通知
T3
T4
通信継続
or
切断？
切断
切断
T5
継続
接続
T6

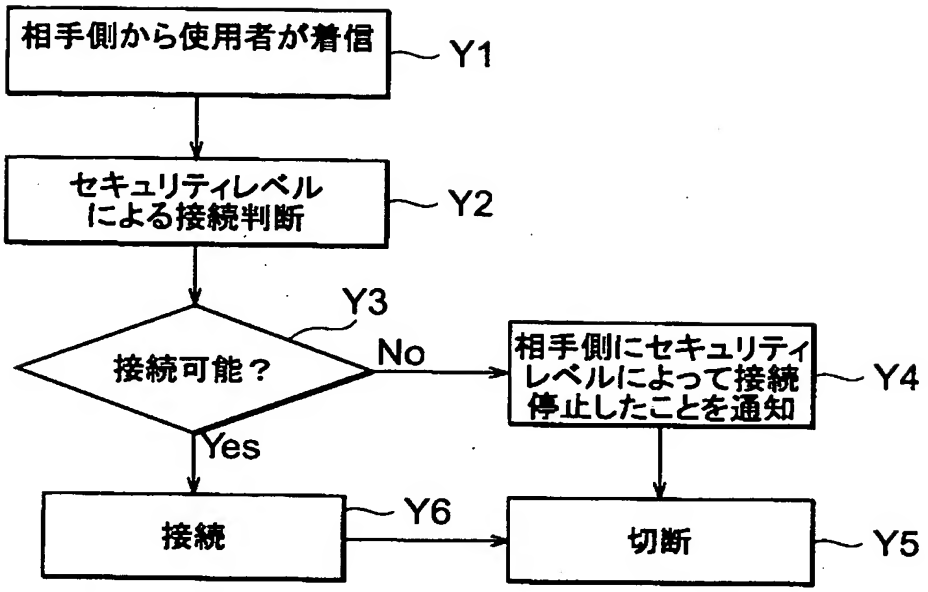
【図６】


使用者がセキュリティ条件を設定(携帯電話装置または使用者情報サーバー)
R1
使用者が発信または、相手側から使用者が着信
R2
R3
セキュリティ条件を満たす？
満たさない
切断
R4
満たす
接続
R5

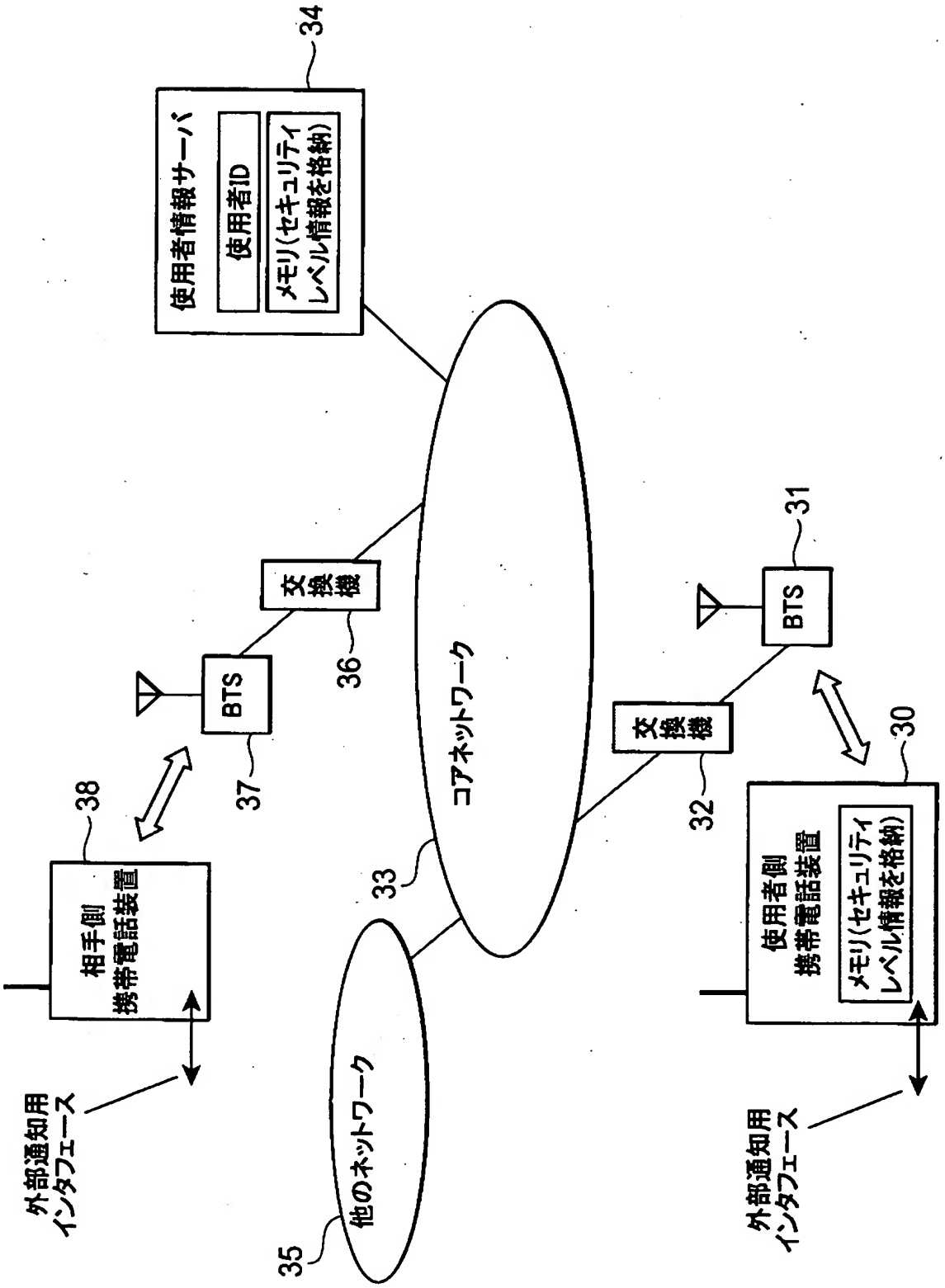
【図７】


使用者がセキュリティ条件を設定(携帯電話装置または使用者情報サーバー)
P1
使用者が発信または、相手側から使用者が着信
P2
通信システムとの通信起動手順開始
P3
P4
セキュリティ条件を満たす？
満たさない
P5
通信継続or切断？
切断
P6
切断
満たす
継続
接続
P8
接続
P7

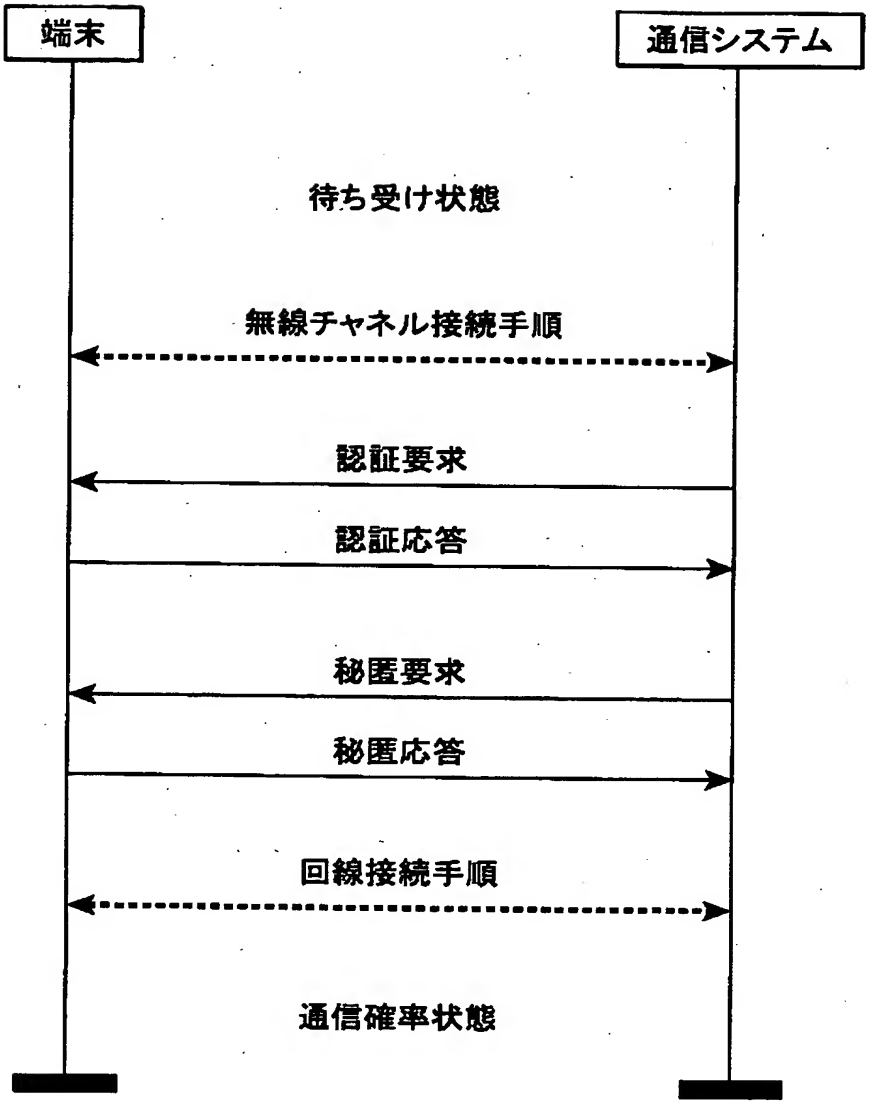
【図８】


相手側から使用者が着信
Y1
セキュリティレベル
による接続判断
Y2
Y3
接続可能？
No
相手側にセキュリティ
レベルによって接続
停止したことを通知
Y4
Yes
接続
Y6
切断
Y5

【図９】


34
使用者情報サーバ
使用者ID
メモリ(セキュリティレベル情報を格納)
交換機
36
BTS
37
38
相手側携帯電話装置
外部通知用インタフェース
35
他のネットワーク
33
コアネットワーク
交換機
32
BTS
31
30
使用者側携帯電話装置
メモリ(セキュリティレベル情報を格納)
外部通知用インタフェース

【図１０】


端末
通信システム
待ち受け状態
無線チャネル接続手順
認証要求
認証応答
秘匿要求
秘匿応答
回線接続手順
通信確率状態

【書類名】　要約書

【要約】

【課題】　接続先のセキュリティレベルに応じて接続可否を選択すること。

【解決手段】　セキュリティ通信機能を有する移動通信端末装置であって、接続先のセキュリティレベルを検出する検出手段４と、検出されたセキュリティレベルを報知する報知手段５とを備える構成を採る。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔３９２０２６６９３〕

１．変更年月日　　２０００年　５月１９日
［変更理由］　名称変更
住　所　　東京都千代田区永田町二丁目１１番１号
氏　名　　株式会社エヌ・ティ・ティ・ドコモ